

# **TALLER INTERNACIONAL Seguridad de la Información ANALISIS DE RIESGO Y CLASIFICACION DE INFORMACION**

**Martin Vila  
2009**

Material que forma parte del Track 1 de Diplomatura Anual en Seguridad de la Información y Auditoría de Sistemas – ISEC INFORMATION SECURITY Inc.

## TRACK 1.1. ANALISIS DE RIESGO Y CLASIFICACION DE INFORMACION METODOLOGIA PRACTICA

### Enfoque a Redes de Informacion

- Metodología Práctica de Implementacion:
  - Clasificacion de la Informacion
  - Redes de Informacion
- Etapas:
  - Identificacion de los componentes
  - Análisis de Riesgos de las Tecnologías
  - Implementacion de las Soluciones
- Estàndares relacionados

# Metodología Práctica de Clasificación de Información

## Etapas

1. Identificación de la información
2. Identificación de los principales riesgos
3. Clasificación de la información teniendo en cuenta los riesgos identificados
4. Difusión a los USUARIOS
5. Mantenimiento y Mejora Continua

# Metodología Práctica de Clasificación de Información

## Etapas

### 1. Identificación de la información

#### Definición de Información

Se considera información a todo dato relacionado con los negocios de la compañía, cualquiera sea su forma y medio de comunicación y / o conservación:

- Formularios / comprobantes propios y/o de terceros
- Información en los sistemas y/o reportes impresos
- Otros soportes magnéticos móviles y/o fijos
- Información transmitida vía oral

## Metodología Práctica de Clasificación de Información

Identificación de los lugares donde se se conserva la información:

- Sistemas aplicativos
- Directorios de red y de estaciones de trabajo
- Correo Electrónico
- Medios Impresos
- Formularios
- Anotaciones
- Equipos

# Metodología Práctica de Clasificación de Información

## 2. Identificación de los principales riesgos

- Captura de PC desde el exterior
- Robo de información
- Spamming
- Violación de e-mails
- Destrucción de equipamiento
- Violación de contraseñas
- Intercepción y modificación de e-mails
- Virus
- Incumplimiento de leyes y regulaciones
- Violación de la privacidad de los empleados
- Ingeniería social
- empleados
- Fraudes informáticos
- Programas "bomba"
- deshonestos
- Interrupción de los servicios
- Destrucción de soportes documentales
- Acceso clandestino a redes
- Robo o extravío de notebooks
- Acceso indebido a documentos impresos
- Software ilegal
- Indisponibilidad de información clave
- Intercepción de comunicaciones
- Falsificación de información para terceros
- Agujeros de seguridad de redes conectadas

## Metodología Práctica de Clasificación de Información

Para facilitar la identificación de los riesgos más críticos se pueden utilizar las siguientes **categorías**:

- Fraudes informáticos
- Ataques externos a las redes
- Modificaciones no autorizadas de datos por empleados
- Acceso y difusión inoportuna de datos sensibles
- Falta de disponibilidad de los sistemas
- Software ilegal
- Falta de control de uso de los sistemas
- Destrucción de información y equipos

## Metodología Práctica de Clasificación de Información

Según su **origen** se pueden agrupar en:

- Naturales
- Intencionales
- No intencionales

Estos riesgos pueden ser clasificados en los siguientes **tipos**:

- Difusión indebida
- Alteración no autorizada
- Falta de disponibilidad

# Metodología Práctica de Clasificación de Información

## Norma ISO 27002 Seguridad de la Información

Preservarla:

**confidencialidad:**

accesible sólo a aquellas personas autorizadas a tener acceso.

**integridad:**

exactitud y totalidad de la información y los métodos de procesamiento.

**disponibilidad:**

acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

## Metodología Práctica de Clasificación de Información

Se debe definir quiénes son los principales **agentes de riesgo** para la información de cada Dueño de Datos:

- Espías comerciales / Competidores
- Empleados deshonestos
- Delincuentes profesionales
- Terroristas informáticos
- Ex-empleados disconformes
- “Hackers”, “Crackers” y similares
- Proveedores
- Clientes
- Operadores Bursátiles
- Compañías asociadas

## Metodología Práctica de Clasificación de Información

Existen distintas metodologías de:

“PONDERACION” de los riesgos según su impacto en el negocio para definir los más altos

“CUANTIFICACION” de acuerdo al impacto económico

En algunos procesos se integra este análisis a los que se realizan en un PLAN DE CONTINUIDAD DEL NEGOCIO, donde se analizan los distintos escenarios de desastres, se identifican los de mayor probabilidad de ocurrencia y se seleccionan los principales.

## Metodología Práctica de Clasificación de Información

### 3. Clasificación de la información teniendo en cuenta los riesgos identificados

1. Análisis de los principales riesgos a la que está expuesta.
2. Categorización en distintos niveles.
3. Aprobación de los sectores / usuarios que deben acceder a la información crítica con permisos
4. Consolidación.

## Metodología Práctica de Clasificación de Información

### 1. Análisis de los principales riesgos a la que está expuesta Riesgos de la Información

El Dueño de Datos / Delgado debe identificar los riesgos a los que está expuesta su información, teniendo en cuenta la posibilidad de que personal interno y/o externo realice:

- divulgación no autorizada
- modificación indebida
- destrucción de los soportes

## Metodología Práctica de Clasificación de Información

### 1. Análisis de los principales riesgos a la que está expuesta

#### Criterios básicos para clasificar la información

El Dueño de Datos / Delegado debe analizar su información para proceder a su clasificación, basándose principalmente en los perjuicios que pudiera ocasionarle a la compañía y/o su personal, el incumplimiento de alguno de los valores generales de seguridad definidos en la Política General.

## Metodología Práctica de Clasificación de Información

### 1. Análisis de los principales riesgos a la que está expuesta

Dichos perjuicios pueden ser:

- Ø económicos,
- Ø financieros,
- Ø políticos,
- Ø sociales,
- Ø de imagen,
- Ø legales y/o
- Ø gremiales.

Complementariamente se deben tener en cuenta las definiciones de las autoridades de la compañía y las leyes y reglamentaciones vigentes.

## Metodología Práctica de Clasificación de Información

### 2. Categorización en distintos niveles

#### Información de acceso público

Toda aquella información que no representa riesgo significativo para la compañía.

#### Información de acceso autorizado

Toda aquella información que puede presentar riesgos para la compañía, y cuyo acceso debe ser expresamente autorizado por el Dueño de Datos / Delegado y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales.

#### Información sensible

Toda aquella información de acceso autorizado que puede presentar riesgos importantes para la Compañía, y que deben cumplir con las siguientes medidas adicionales a las definidas para acceso autorizado.

## Metodología Práctica de Clasificación de Información

### 2. Categorización en distintos niveles

Tener en cuenta también los criterios de seguridad a aplicar para cada tipo de información definidos en la normativa respectiva para cada “momento” o “proceso” de la información:

- Autorización
- Conservación
- Envíos
- Impresión
- Divulgación a terceros
- Destrucción

## Metodología Práctica de Clasificación de Información

### 2. Categorización en distintos niveles

Considerar también el sentido de “OPORTUNIDAD” teniendo en cuenta que la información tiene distinta criticidad en distintos momentos.

## Metodología Práctica de Clasificación de Información

### 3. Aprobación de los sectores / usuarios que deben acceder a la información crítica con permisos

- Definir los USUARIOS de la Información:
  - Por PUESTOS / Perfiles
  - Por Grupos de afinidad
  - Por Usuarios Específicos
- Definir el sistema de Permisos a otorgarles:
  - Solo Lectura
  - Modificación
  - Distribución
  - Destrucción
- Asignar los permisos

## Metodología Práctica de Clasificación de Información

### 4. Consolidación

- Integrar los entregables de cada Dueño de Datos
- Identificar inconsistencias
- Acuerdos entre Dueños de Datos
- Mediación del Foro / Comité
- Soluciones alternativas

## Metodología Práctica de Clasificación de Información

### 4. Difusión a los USUARIOS

Integrarlo con el proceso de Concientización de USUARIOS:

- Usuarios finales
- Terceros y personal contratado

## Metodología Práctica de Clasificación de Información

### 5. Mantenimiento y Mejora Continua

- Definir el período de actualización
- Efectuar la actualización
- Reportes de los cambios

ISO 27002: Revisiones periódicas de:

- Riesgos
- Controles implementados

# Metodología Práctica de Clasificación de Información

Detalle de la información	Riesgos			Clasificación			SOPORTE					PERMISOS			COMENTARIOS
	Confid	Integ	Dispon	Uso Público	Acceso Autorizado	Sensible	Red	Aplicativo	PC	CD/DK T	Impresos	TOTAL	SOLO LOCAL	SOLO CONSULTA	

**Alcance:**

**Con que nos encontramos?**

**Principales Componentes de  
una red de información**

# Principales Componentes de una red de información

- **CAPA FISICA**
- **DISPOSITIVOS DE NETWORKING Y COMUNICACION**
- **SISTEMAS OPERATIVOS;**
- **BASES DE DATOS**
- **CORREO ELECTRONICO Y MENSAJERIA**
- **SERVIDORES WEB**
- **APLICACIONES DE NEGOCIO**
- **OTRAS TECNOLOGIAS RELACIONADAS**

# Metodología Práctica de Implementación:

- **Procesos** (CONTROLES DE GESTION)
  - Alcance de TI
  - Segregacion de Funciones
  - Procesos detallados
  - Identificacion de Controles
  - Gap, Implementacion, Mejora Continua

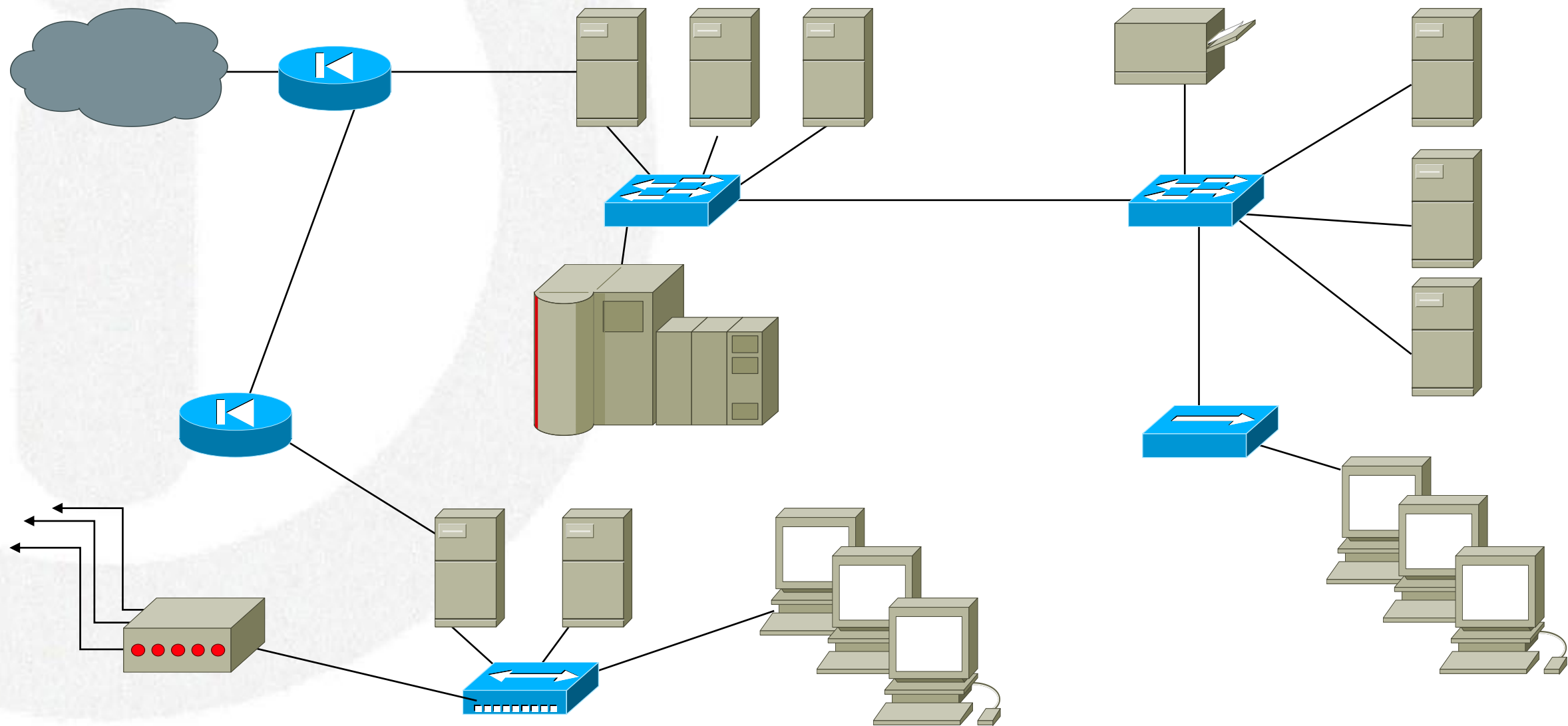
## Metodología Práctica de Implementación:

- **Seguridad Logica** (CONTROLES TECNICOS)
  - Diseño de la Red
  - Selección de soluciones
  - Documentacion
  - Implementacion
  - Mantenimiento
  - Monitoreo
  - Actualizacion, Mejora Continua

# Metodología Práctica de Implementación: ETAPAS

- **Seguridad Logica** (CONTROLES TECNICOS)
  - Diseño de la Red
  - Selección de soluciones
    - Identificación de los componentes
    - Análisis de Riesgos de las Tecnologías
    - Implementación de las Soluciones

# Identificación de los Componentes de una Red



## Principales Componentes de una red

- Servidores
- Servidores de Usuarios
- Servidores de Archivos
- Servidor de Aplicaciones
- Servidor de Servicios
- Servidor DNS
- Servidores de Correo
- Servidores de Base de datos
- Servidores Antivirus
- Servidor Proxy
- Servidor RADIUS
- Servidores de Datawarehouse
- Servidores de WEB
- Servidores de Back Up
- Servidores de Impresión
- Servidores de Encriptación
- Servidores de Control de Maquinarias
- Estaciones de trabajo de usuarios
- Notebooks
- Hubs /Switches
- Router

Acceso Remoto (RAS, VPN, Terminal Server)

Firewall / IDS / IPS

Dispositivos Mviles (cd, dkt, flash memories, etc)

Dispositivos de Autenticacion (Biométricos, Tokens, Smart Cards, etc)

Telefonía (centrales telefonicas, voicemail, Voz sobre IP)

Cámaras IP

Wireless 802.11, Bluethoot e Infrarrojos

Impresoras /Fotocopiadoras /Scanners

Celulares (Analógicos, Digitales, GSM, GPRS)

Camaras Digitales

Dispositivas para Videoconferencias

Lectoras de Código de Barras (Alambrica e Inalámbrica)

PDA/Tablet PC

UPS

Honey Pots / Honey Nets

# Análisis de Riesgos de las Tecnologías:

- **Riesgos de C I D** (Confidencialidad, Integridad, Disponibilidad)
- **Probabilidad de Ocurrencia**
- **Valoracion del Activo**

# Análisis de Riesgos de las Tecnologías:

- **PASOS A SEGUIR:**
  - Selección de la metodología de Ponderación (Ej: 1 a 5, 1 a 10, Alta/Media/Baja)
  - Identificación del **ACTIVO**
  - Aplicación del criterio ( $R \times P \times VA$ )
  - Identificación del Riesgo Valorizado
  - Clasificación de las **ZONAS de RIESGO** (Rojo/Amarillo/Verde)

# Implementacion de las Soluciones:

- **PASOS A SEGUIR:**
  - **Identificacion de los tipos de SOLUCIONES:**
    - **TECNICAS (Software / Hardware / Integradas)**
      - IDENTIFICACION
      - AUTENTICACION
      - AUTORIZACION
      - NO REPUDIO
      - ENCRIPTACION
      - ANTI-XXXX (virus, spam, Spyware, Phishing...)

# Implementacion de las Soluciones:

- **TECNICAS (Software / Hardware / Integradas)**
  - **MONITOREO**
  - **AUDITORIA**
  - **DETECCION / ESCANEOS**
  - **FORENSE**
  - **BALANCEO DE CARGA**
  - **REDUNDANCIA / CLUSTERING**
  - **ADMINISTRACION CENTRALIZADA**
  - **AUTENTICACION REMOTA**
  - **GESTION DE IDENTIDADES**
  - **CONTROL DE CONTENIDOS**
  - **HONEYPOTS**
  - **CERTIFICADOS / FIRMAS DIGITALES**
  - **VPN**
  - **GESTION DE INCIDENTES**
  - **BIOMETRIA**
  - **RFID**

# Implementacion de las Soluciones:

- **GESTION**
  - PERSONAS ( Ej, CONVENIOS CONFIDENCIALIDAD)
  - PROCEDIMIENTOS
  - Otros
- **SEGURIDAD FISICA**

# Implementacion de las Soluciones:

- Relacionar los tipos de SOLUCIONES con las ZONAS DE RIESGOS:
  - Identificar la MEJOR Solucion (Maxima/Optima/Minima) para cada Zona de Riesgo
  - Ponderar su IMPLEMENTACION:
    - Mandatorio
    - Buenas Practicas
    - Opcional
  - Nota: Matriz de Madurez de Controles (Ej COBIT: 1 a 5)

# Metodología Práctica de Implementación: ETAPAS

- **Seguridad Logica** (CONTROLES TECNICOS)
  - Diseño de la Red
  - Selección de soluciones
  - Documentacion
  - Implementacion
  - Mantenimiento
  - Monitoreo (ej, Tableros de Control)
  - Actualizacion, Mejora Continua

## Estandares Relacionados:

- Gestion (ISO27002, COBIT, ITIL, RBAC, ISMR3, ISSAF, etc)
- Tecnicos (MODELO OSI, OSSTMM, OWASP, PCI, etc)
- RFCs
- Propios de los Proveedores de las Tecnologias

Muchas Gracias  
Martin Vila  
[www.isec-global.com](http://www.isec-global.com)